EITDR Question C9 - "Does your IT investment process/store Privacy Act Information (i.e., social security number, personal data, etc)?"
EITDR Question C10 - "Is a Privacy Act Information Assessment (PIA) required?"

Note that a Privacy Impact Assessment (PIA) is required only when ***all*** of the following conditions are met:
(1) personally identifiable information is collected (e.g. Social Security numbers, fingerprints, etc), and
(2) the information is collected from the general public (DoD contractors are considered by the Office of the Secretary of Defense's Chief Information Officer to be members of the general public, but military members and DoD government employees are not), and
(3) the information is collected from 10 or more members of the general public, and
(4) the investment is "IT" and not a National Security System (NSS as reflected in EITDR question G58, which occurs when "Yes" is given for at least one of the EITDR questions G59 through G64).

Answering at least one of the following EITDR questions makes an investment a "National Security System", which is exempted from needing a Privacy Impact Assessment:
- G59 Does the function, operation, or use of the system/investment involve intelligence activities?
- G60 Does the function, operation, or use of the system/investment involve cryptologic activities related to national security?
- G61 Does the function, operation, or use of the system/investment involve command and control of military forces?
- G62 Does the function, operation, or use of the system/investment involve equipment that is an integral part of a weapon or weapons system?
- G63 If the use of the system/investment is not routine administrative or business applications, is the system/investment critical to the direct fulfillment of military or intelligence missions?
- G64 Does the system/investment store, process, or communicate classified information?

Here are a few examples to clarify:
- If an IT investment collects digitized handprints only from DoD military and government employees, no Privacy Impact Assessment is required since no members of the general public are involved.
- If an IT investment collects names and birthdates from DoD government employees and DoD contractors, a Privacy Impact Assessment is required because DoD contractors are considered to be members of the general public.
- If an investment collects Social Security numbers from students for possible recruitment, civilian dependents of a military member for base housing, performers visiting a base for a heritage month celebration, members of a nonprofit organization for an Air Show, etc, but that same investment also processes classified information, that investment is considered to be a "National Security System" and not an "IT investment"; therefore, no Privacy Impact Assessment is required.

A Privacy Impact Assessment (PIA - http://www.whitehouse.gov/omb/memoranda/m03-22.html) should not be confused with a System of Records Notice (SORN - http://www.whitehouse.gov/omb/memoranda/m99-05-b.html). A PIA informs the public how personally identifiable information is collected, stored, protected, shared, and managed in order to show that investment owners/developers have consciously incorporated privacy protections throughout the entire life cycle of the IT investment. A SORN informs the public that personal identifier and personal data (retrieved by the personal identifier) are being collected, what is being collected, why it is being collected, and under what authority it is being collected. PIAs are usually published on a Federal agency's website (e.g. http://www.foia.af.mil/Privacy/PrivImpAssess.shtml , http://www.irs.gov/privacy/article/0,,id=122989,00.html , http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm) while SORNs are usually published in the Federal Register (http://www.archives.gov/federal-register/ and for DoD SORNs, also at http://www.defenselink.mil/privacy/notices/).

There is no exhaustive list of Privacy Act information. Some examples are:
- Marital status (single, divorced, widowed, separated)
- Number, name, and sex of dependents
- Civilian educational degrees and major areas of study (unless the request for the information relates to the professional qualifications for Federal employment)
- School and year of graduation
- Home of record
- Home address and phone
- Age and date of birth (year)
- Present or future assignments for overseas or for routinely deployable or sensitive units
- Office and unit address and duty phone for overseas or for routinely deployable or sensitive units
- Race/ethnic origin
- Educational level (unless the request for the information relates to the professional qualifications for Federal employment)
- Social Security Number
- Mother's maiden name
- Biometric records like digitized fingerprints, palm prints, retina scans, voice patterns, face scans, handwriting, etc
- Email address
- Vehicle registration plate number
- Driver's license number
- Credit/Debit card numbers like the Government Travel Card, IMPAC Card, etc
- Criminal record
- Account numbers used in banks, stock brokerage firms, Thrift Savings Plan, other financial institutions
- And other data including any other personal information which is linked or linkable to an individual. Use your best judgment - can someone off the street identify (or trace back to) a specific person after viewing the information in the IT investment?